CLAIMS

We claim:

1. A method of operating an intrusion detection system, the method comprising the steps of:

determining a present alert generation rate of an intrusion detection system;

comparing the present alert generation rate with an alert generation rate threshold; and

altering an element of a signature set of the intrusion detection system responsive to an outcome of the step of comparing.

2. A method of operating an intrusion detection sensor, the method comprising the steps of:

determining a present alert generation rate of an intrusion detection sensor;

comparing the present alert generation rate with an alert generation rate threshold; and

when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of the intrusion detection sensor to decrease an alert generation rate of the intrusion detection sensor.

3. The method of claim 2, wherein the element is a signature threshold quantity.

4. The method of claim 2, wherein the element is a signature threshold interval.

5. A method of operating an intrusion detection system, comprising the steps of:

monitoring for occurrence of a signature event; and

when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity; and

when the value of the signature event counter exceeds the signature threshold quantity, generating an alert, recording a time of generating the alert in a log, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold; and

when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of an intrusion detection system to decrease an alert generation rate of an intrusion detection sensor.

6. The method of claim 5, wherein the element is a signature threshold quantity.

7. The method of claim 5, wherein the element is a signature threshold interval.

8. Programmable media containing programmable software for operation of an intrusion detection system, programmable software comprising the steps of:

determining a present alert generation rate of an intrusion detection system;

comparing the present alert generation rate with an alert generation rate threshold; and

altering an element of a signature set of the intrusion detection system responsive to an outcome of the step of comparing.

9. Programmable media containing programmable software for operation of an intrusion detection sensor, programmable software comprising the steps of:

determining a present alert generation rate of an intrusion detection sensor;

comparing the present alert generation rate with an alert generation rate threshold; and

when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of the intrusion detection sensor to decrease an alert generation rate of the intrusion detection sensor.

10. Programmable media containing programmable software for operation of an intrusion detection system, programmable software comprising the steps of:

monitoring for occurrence of a signature event; and

when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity; and

when the value of the signature event counter exceeds the signature threshold quantity, generating an alert, recording a time of generating the alert in a log, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold; and

when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of an intrusion detection system to decrease an alert generation rate of an intrusion detection server.

11. The programmable media of claim 10, wherein the element is a signature threshold quantity.

12. The programmable media of claim 10, wherein the element is a signature threshold interval.